REGENTS' POLICY
PART II - ADMINISTRATION
Chapter 02.07 - Information Resources

P02.07.010. General Statement: Information Resources.

Within the limits of facilities, resources, and personnel, the university shall establish, through university regulation, and MAU rules and procedures, a framework for access to, and the responsible use of, university information resources.

(02-18-00)

P02.07.020. Information Resources Definitions.

A. In this chapter

1. "information resources" includes the systems and networks owned, leased, or operated by the university, as well as the software and data resident on the systems and networks; and

2. "user" means an individual, including but not limited to, students, faculty, staff and affiliates, who accesses, transmits or stores data on information resources

B. Other definitions for this chapter may be established in university regulation.

(02-18-00)

P02.07.030. Objectives for Management of Information Resources.

Information resources shall be managed in a manner that will:

A. respect First Amendment rights and privacy, including academic freedom;

B. reasonably protect against misrepresentation, tampering, destruction, liability and theft of intellectual efforts;

C. maintain the integrity of university information resources;

D. allocate finite resources based on prioritized needs; and

E. protect the confidentiality of sensitive data collected under research grants and contracts with outside agencies.

(02-18-00)

P02.07.066. Mobile Device Security.

A. University employees and students using a laptop computer or mobile device (e.g. portable hard drives, USB flash drives, smartphones, tablets) are responsible for the university data stored, processed or transmitted via that computer or mobile device and for following the security requirements set forth in this policy and other applicable information resources policies and regulations regardless of whether that device is the property of the university or the individual.

B. The use of unprotected mobile devices to access, store, manipulate or transmit university non-public information as defined in R02.07.094 is prohibited regardless of whether or not such equipment is owned or managed by the university.

C. The chief information technology officer is responsible for coordinating with the campuses in the development of consistent measures and business practices for ensuring the security of non-public data on mobile devices.

Reference: Alaska Statutes Chapter 45.48 Personal Information Protection Act

(02-19-15)

P02.07.070. Administrative Responsibilities.

A. An MAU may establish rules and procedures to define conditions and enforcement mechanisms for use of information resources under its control. MAU statements must be consistent with this policy and university regulation and published in a manner reasonably designed to make these conditions known to users.

B. The university reserves the sole right to limit, restrict or extend access to its information resources.

(02-18-00)

UNIVERSITY REGULATION
PART II – ADMINISTRATION
Chapter VII – Information Resources

R02.07.010. General Statement – Information Resources.

MAUs shall establish rules and procedures for the management of information resources in accordance with regents' policy and university regulation.

(01-31-01)

R02.07.020. Information Resources Definitions.

In this chapter and, under the authority of P02.07.020.B, in regents' policy, unless the context requires otherwise,

A. "director of information resources" means the senior person with direct management responsibilities for information resources at an MAU, or that person's designee during periods of absence;

B. "information resources" means the information systems and information networks owned, leased, or operated by the university, regardless of the source of funding, and includes the data, software and other information resident on systems or carried over networks; in addition to this chapter, this definition applies to all information resources acquired and controlled by:

1. system administration, the financial, human resource, and student information systems operated for the entire university system;

2. university campuses, the campus-

D. “information system” means the entire suite of hardware, software, data, and network connections that stores, manipulates, and disseminates, usually over a data network, a particular category of information;

E. “manager” means a person with responsibility or authority for a particular information resource; manager responsibilities include determining access privileges of users, the procedures for input, integrity, or dissemination of data, and security measures protecting the resource;

F. “network” means the physical infrastructure that carries voice, video and data within an MAU up to and including connections to external networks or providers; a network includes switches, routers, firewalls, store and forward devices, software used to manage

2.

the information might be further disclosed in an appropriately confidential manner."

(01-31-01)

R02.07.044. Granting or Denial of Access.

Access to information resources will be granted or denied to university units, faculty, staff, students, and affiliates based upon relevant factors, including protection of intellectual property rights, legal and contractual obligations, security, privacy, the individual's need for the information or for access to the resource, and the risk of damage to, liability of, or loss by, the university.

(01-31-01)

R02.07.046. Temporary Suspension or Restriction of Access.

A. Pursuant to the guidelines set out in this section, information resources personnel may temporarily suspend or restrict access to information resources to which a particular university unit, individual, or class of individuals would otherwise have access.

B. Only persons with written authority to do so may temporarily suspend or restrict access.

C. The suspension or restriction should be no greater in scope or duration than is appropriate to protect information resources.

D. A prompt attempt should be made, when appropriate, to resolve the circumstances giving rise to the suspension or temporary restriction by making an explicit request to the user subject to the suspension or temporary restriction consistent with preserving the integrity and utility of the information resource.

E. Persons suspending or restricting access should promptly refer unresolved issues related to suspension or temporary restriction of access to appropriate MAU authorities for long term resolution and possible discipline.

(01-31-01)

R02.07.048. Disciplinary Action for Unauthorized Access or Disclosure.

C. respect copyright and other intellectual property rights; copying files or passwords belonging to others or to the university may violate copyright law or constitute plagiarism or theft; software licensed by the university or otherwise resident on university equipment must be used in accordance with any applicable license agreement; violations of the terms of software license agreements are not within the scope of university employment and constitute misconduct; the university may require violators to reimburse and pay fines or damages and impose disciplinary action up to and including dismissal from employment or expulsion from the university;

D. know that any modification of information resources without authorization, including altering data, introducing viruses, or damaging files is prohibited;

E. clearly and accurately identify the author in all communications; concealment or misrepresentation of an author's name or affiliation to mask irresponsible or offensive behavior is a serious abuse; appropriating the identifiers of other individuals to misrepresent authorship or ownership constitutes fraud;

F. obtain authorization to access information resources as established in MAU rules and procedures or by the information resource personnel with authority to manage the information resource;

G. maintain the integrity of passwords and other security technologies; users must not evade, disable, or crack password or other security provisions; or circumvent, alter, or disable access permissions, records of them, or technologies implementing access restrictions; users must not share individual account passwords;

H. use resources efficiently and adhere to limitations or restrictions on computing resources, such as storage space, time limits, or amount of resources consumed, when asked to do so by the managers of information resources; objections to such restrictions may appropriately be brought to the proper authority, but this does not remove the user's obligation to adhere to restrictions in force;

I. recognize the limitations on privacy inherent within the electronic environment and know that

1. intended security of electronic files may be compromised;

2. network communications and the actions of users on many shared information systems are routinely logged and archived;

3. information "deleted" by users may nevertheless be preserved in routine backup files, archives, or audit trails;

4. information resources personnel may view the contents of files as part of their responsibilities;

E. The Alaska Executive Branch Ethics Act does not apply to students in their capacity as students.

(01-31-01)

R02.07.054. Content Restrictions.

Managers of information resources may impose on shared information resources under their management constraints and measures designed to maintain system functionality and to assure data integrity and security. Such constraints and measures may lead to limits or restrictions on some types of activities. Restrictions based solely on the content of information must not conflict with the academic mission of the university and right to individual freedom of expression. Content restrictions are thus appropriate only in specific limited circumstances, such as the following:

A. Limited-Public Forums

Limited-public forums, as distinguished from private communication or public forums, may have content restrictions so long as they are based on topic rather th1W*ne.orums

G. Information resources personnel may not access the content of electronic communications or copy or examine any files or other information resident on or processed through information resources except as authorized by A. of this section or upon a valid request made in accordance with regents' policy or university regulation, or as required by state or federal law.

(01-31-01)

R02.07.065. Security Breach Involving Personal Information.

The regulation regarding security breaches involving personal information is located in Regulation 05.08.023.

(08-30-07)

R02.07.066. Mobile Device Security

A. Protection of Non-Public Information

1. The proper personnel within the university need to be made aware of the loss of university non-public information accessed through, stored within, manipulated by, or transmitted to, its information resources. In some instances the University has a duty to report loss of information to third parties. Therefore faculty, staff, students, affiliates, and others with access to university information resources are required to protect non-public information to which they have access and report any loss of control of that information.

2. Every user of computer equipment, including laptop computers or other mobile devices (e.g. portable hard drives, USB flash drives, le

F. Additional Requirements.

In addition to appropriate information handling requirements determined by the general data classification under Regents' Policy Chapter 02.07 – Information Resources and university regulation, sector-specific data (e.g., Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), etc.) may have additional requirements. Individual divisions, schools, colleges, Institutes or departments may impose additional information security requirements beyond those set forth in this regulation and as may be required by sponsors, government agencies or other external entities. Users should check with the Statewide Office of Information Technology for assistance.

G. Requirements When Traveling Overseas

University personnel and students carrying university-issued laptops or mobile devices while traveling abroad, whether on business or for pleasure, must comply with data protection measures in this regulation, with U.S. trade control laws, with University Regulation 10.07.035 – Export Control Licensing, and with the laws of the destination country. U.S. export control laws may prohibit or restrict such activities absent special U.S. government licenses. For current guidance on traveling abroad with a laptop or other

B. safeguard the integrity and confidentiality of information to a reasonable and economically feasible degree consonant with the nature of the information in the resource;

C.

R02.07.074. System Administrator Responsibilities.

A. System administrators have unique privileges and responsibilities including the following:

1.

5. system administrators shall configure software systems so as to facilitate the confidentiality of User communication;

6. system administrators shall stay abreast of any vulnerabilities of their systems and manage security in accord with appropriate recommendations; system administrators are responsible for remaining up-to-date with security issues relevant to the systems they administer, including vendor information channels and computer emergency response team bulletins;

7. system administrators should configure their systems to minimize the chance for abuse, and act promptly to end abuses upon notification.

B. Except as authorized by these regulations, system administrators shall not compile or log information on information systems for which they do not have administrative responsibilities.

(08-25-14)

R02.07.080. No Rights of Actions Against the University.

Nothing in this chapter is intended to create, extend, or support any cause of action or other claim for damages against the university or its employees acting within the scope of their employment.

(01-31-01)

R02.07.090. Data Classification Standards: General Statement

The University of Alaska (UA) generates, acquires, and maintains a large number of electronic records. In addition, UA often enters into relationships with third parties who maintain electronic records and information associated with these relationships. UA, as well as its affiliates, are often legally required to limit access to, distribution of, and/or disclosure of electronic records and information. The approach at UA is to adopt a classification scheme for all data.

(08-27-09)

R02.07.091. Data Classification Standards: Purpose

Data classification standards help personnel who own and maintain information resources and systems to determine the sensitivity of the data within those systems. This regulation is designed to prevent the following:

--Unauthorized internal access to electronic information
--Unauthorized external access to electronic information
--Illegal or otherwise inappropriate use of UA electronic information
--Loss, corruption, or theft of UA electronic information

(08-27-09)